CLOUDSWITCHED

FREE RESOURCE — IT RISK ASSESSMENT TEMPLATE

IT Risk Assessment Template

A structured framework for identifying, scoring and treating the IT risks that threaten a UK SME. Capture every risk, rate likelihood and impact, decide on treatment, and assign owners and deadlines — the audit-ready record cyber insurers, Cyber Essentials assessors and your board all want to see.

6	5×5	25+	Fillable
ASSESSMENT SECTIONS	LIKELIHOOD × IMPACT MATRIX	CONTROL CHECKS COVERED	TICK & TYPE IN ANY VIEWER

ISO 27005 ALIGNED · CYBER ESSENTIALS · BOARD-READY · AUDIT-READY

PREPARED FOR	PREPARED BY	VERSION	FORMAT
Cloudswitched Knowledge Library	Cloudswitched Ltd.	2026 Edition	Interactive PDF

00

How to use this template

Use this template once a year, and again after any material change to systems, suppliers, headcount or premises. Walk through the six sections in order, populate the risk register, score each risk on the 5×5 likelihood×impact matrix, score your controls Y/N/N-A, and write a treatment action for every Medium-or-above risk. This is an **interactive PDF** — tick boxes and type into the fillable lines directly in any modern viewer.

WHAT THIS TEMPLATE IS

A board-ready, audit-ready record of the IT risks facing your organisation, how they are being treated, who owns the treatment, and by when. It aligns with **ISO 27005** language for risk identification, analysis, evaluation and treatment, and it generates the evidence cyber insurers, Cyber Essentials Plus assessors and ICO investigators expect to see.

RISK ACCEPTANCE IS A BOARD DECISION — NOT AN IT DECISION

Any risk scored **High (12+) or Critical (16+)** that you intend to *accept* rather than treat must be signed off by a director. Document the rationale on page 07. Silent acceptance of a critical risk — "we knew but did nothing" — is the single most damaging finding in a breach investigation or insurance dispute.

The six assessment sections

- **01 Scope & assessor details** — organisation, assessor, review date, what is in and out of scope.
- **02 Risk scoring methodology** — 1-5 likelihood and impact scales, the 5×5 heat-map.
- **03 Risk register** — every identified risk with ID, owner, L × I score and target date.
- **04 Control assessment** — Y / N / N-A checks against 25+ baseline IT controls.
- **05 Risk treatment plan** — treat / transfer / accept / avoid action for each Medium-or-above risk.
- **06 Sign-off & review schedule** — named approver, date, next review.

The four treatment options

Every risk in the register lands on one of four strategies. State the choice explicitly — ambiguity here is what kills audits.

- **Treat** — reduce likelihood or impact with a control or process change. The default for Medium-and-above risks.
- **Transfer** — move the risk to a third party (cyber insurance, outsourced SOC, vendor SLA with credits).
- **Accept** — a deliberate, director-signed decision to live with the risk. Document the rationale.
- **Avoid** — remove the underlying activity, system or supplier entirely.

01

Scope & assessor details

Capture the basic provenance of this assessment first. The scope statement matters: it sets the boundary for everything that follows — risks outside scope are not just ignored, they are *explicitly out of scope* with a named reason.

Organisation

Organisation name _____

Trading address _____

Industry / sector _____

Headcount (approx.) _____

Assessment

Assessment reference _____

Date of assessment _____

Lead assessor _____

Reviewing director _____

Version of this register _____

Next review date _____

Scope statement

Describe what is **in scope** — sites, business units, systems, suppliers, data domains — and what is **explicitly out of scope** with the reason.

_____

_____

_____

KEEP THE SCOPE HONEST

Risks you decide not to assess are still risks. List them out of scope with the name of the register or programme that does cover them — "we forgot" is not a defence in a board review or an insurance claim.

02

Risk scoring methodology

Every risk in the register is scored on two 1-5 scales: **Likelihood** (how plausible is the event in the next 12 months?) and **Impact** (how bad if it happens?). The product L × I gives a raw score 1-25, which maps to one of four bands — Low, Medium, High, Critical.

Likelihood scale (1-5)

SCORE		DEFINITION — IN THE NEXT 12 MONTHS
1	**Rare**	Highly unlikely. No recent precedent in the organisation or sector.
2	**Unlikely**	Could occur but not expected. Sector-level incidents but never us.
3	**Possible**	May happen at some point. Has happened once historically or to similar firms.
4	**Likely**	Will probably occur. Active threat or recurring near-miss observed.
5	**Almost certain**	Expected to occur. Already happening or imminent.

Impact scale (1-5)

SCORE		DEFINITION — IF THE EVENT OCCURS
1	**Negligible**	Minor inconvenience. < 1 hr disruption. No data loss. No regulator interest.
2	**Minor**	Half-day disruption. Limited data exposure. Internal-only impact.
3	**Moderate**	1-day disruption. Customer-visible. Potential regulator notification.
4	**Major**	Multi-day outage. Confirmed breach. ICO 72-hr clock. Insurance claim.
5	**Severe**	Existential. Week+ outage, mass data loss, regulator action, viability at risk.

Score bands

`1-5 LOW`	Monitor. Document and review at the next annual cycle. No active treatment required.
`6-11 MED`	Treat. Assign an owner and a target completion date within 6 months.
`12-15 HIGH`	Treat urgently. Owner + target date within 90 days. Director awareness.
`16-25 CRIT`	Treat immediately. Board-level escalation. Target within 30 days or formal acceptance.

03

Risk register

List every identified IT risk on its own row. Use a stable, sequential ID (R001, R002 ...) you will reuse on the treatment plan and in future revisions of this register. Score each risk on the 1-5 likelihood and impact scales from section 02; the Score column is L × I.

ID	RISK DESCRIPTION	L	I	SCORE	OWNER	TARGET DATE

COMMON IT RISK CATEGORIES — PROMPT LIST

Ransomware & malware · phishing / business-email compromise · insider misuse · lost or stolen device · unpatched systems · weak / shared credentials · cloud misconfiguration · backup failure or untested restore · single-supplier dependency · key-person dependency · data-centre or office power / internet outage · GDPR breach · expired SSL / domain · shadow IT · M&A integration risk · supplier insolvency.

04

Control assessment

Score each baseline IT control against your environment. Tick **Y** if the control is in place and operating, **N** if it is not, or **N-A** if it does not apply to your scope (state the reason in section 05). Every **N** is a candidate risk for the register on page 04.

Access & identity

MFA enforced on all admin and remote-access accounts (privileged users, VPN, RDP, M365 admin).	☐ Y	☐ N	☐ N-A
MFA enforced on all end-user cloud accounts (Microsoft 365, Google Workspace, SaaS apps).	☐ Y	☐ N	☐ N-A
Joiner / mover / leaver process documented and followed, with same-day deprovisioning on exit.	☐ Y	☐ N	☐ N-A
Privileged accounts **separate from daily accounts**, with logged use and quarterly review.	☐ Y	☐ N	☐ N-A
Password policy meets NCSC guidance (12+ chars, no forced rotation, banned-list, password manager available).	☐ Y	☐ N	☐ N-A

Endpoint & network

EDR / antivirus deployed on every endpoint with central console and managed alerts.	☐ Y	☐ N	☐ N-A
OS & application patches applied within 14 days of release; critical CVEs within 48 hours.	☐ Y	☐ N	☐ N-A
Disk encryption enabled on every laptop, desktop and removable drive (BitLocker / FileVault).	☐ Y	☐ N	☐ N-A
Firewall with managed rule-base, default-deny inbound, and quarterly rule review.	☐ Y	☐ N	☐ N-A
Guest / IoT network segregated from corporate VLANs with no route into production.	☐ Y	☐ N	☐ N-A

04

Control assessment (continued)

Data, backup & resilience

3-2-1-1-0 backups in place: three copies, two media, one off-site, one immutable, zero errors on last test.	☐ Y	☐ N	☐ N-A
Restore test performed and documented within the last 90 days for critical systems.	☐ Y	☐ N	☐ N-A
RPO & RTO defined per critical system and agreed with the business owner.	☐ Y	☐ N	☐ N-A
Personal data inventory maintained and aligned to the GDPR Article 30 record of processing.	☐ Y	☐ N	☐ N-A
DR / business continuity plan documented, tested in the last 12 months, and known to the response team.	☐ Y	☐ N	☐ N-A

Monitoring, response & suppliers

Security logging centralised (SIEM / cloud logs) with retention ≥ 12 months and alerting on key events.	☐ Y	☐ N	☐ N-A
Incident response plan documented with roles, escalation tree and ICO 72-hr decision flow.	☐ Y	☐ N	☐ N-A
Vendor risk review on every critical supplier with DPA, ISO/SOC certification check, and exit plan.	☐ Y	☐ N	☐ N-A
Cyber insurance policy held, current, and key warranties (MFA, EDR, backups) verified to be true.	☐ Y	☐ N	☐ N-A
Cyber Essentials (or Plus) certification current; gaps identified and tracked.	☐ Y	☐ N	☐ N-A

People & awareness

Annual security awareness training completed by 100% of staff, with completion tracked.	☐ Y	☐ N	☐ N-A
Phishing simulations run quarterly; click-rate trended and remediation training assigned.	☐ Y	☐ N	☐ N-A
Acceptable use & remote-working policies signed by all staff and reviewed annually.	☐ Y	☐ N	☐ N-A

05

Risk treatment plan

For every risk on the register scored Medium-or-above, record the treatment decision (**Treat / Transfer / Accept / Avoid**), the action that closes it, the named owner, and the target completion date. The Risk-ID column ties the treatment back to the risk register on page 04.

RISK ID	STRATEGY	TREATMENT ACTION	OWNER	DEADLI

Accepted risks — director rationale

List any risk you have chosen to **accept** rather than treat. State the risk ID, the reason for acceptance, and the director who signed off. This record is what protects the organisation in a post-incident enquiry.

OWNERS AND DATES — NOT ASPIRATIONS

A treatment action without a named owner is a wish; without a real deadline it is procrastination. Every High or Critical entry should have both, or it should be formally moved to the Accept column and signed off above.

06

Sign-off & review schedule

The assessment is complete only when a named assessor and a director have signed it off, and a calendar entry exists for the next review. Without that final step, this is a draft — not a board-ready record.

Review schedule

Date of this assessment _____

Next full review (12 months) _____

Trigger events for early review _____

Calendar entry created (Y/N) _____

Summary statement

Provide a one-paragraph summary for the board: how many risks, how many High/Critical, headline treatment actions, residual risk position.

_____

_____

_____

PREPARED BY	DATE	APPROVED BY (DIRECTOR)
_____	_____	_____

CLOUDSWITCHED

IT RISK & CYBER RESILIENCE

info@cloudswitched.com

New London House, 6 London St
London EC3R 7LP · United Kingdom